

Polar Grassmannians and Their Codes

Ilaria Cardinali and Luca Giuzzi

December 12, 2014

Abstract

We present a concise description of Orthogonal Polar Grassmann Codes and motivate their relevance. We also describe efficient encoding and decoding algorithms for the case of Line Grassmannians and introduce some open problems.

1 Introduction

The aim of this talk is to survey some recent results on Polar Grassmann codes and propose some open problems which we are currently considering.

Polar Grassmann codes have been introduced in [3] as the projective codes arising from the Plücker embedding ε_k of an orthogonal Grassmannian $\Delta_{n,k}$.

The abstract is organized as follows: in Section 2 we provide some quick background on orthogonal Grassmannians and describe some of the projective codes they determine. Section 3 introduces an enumerator which might be use to implement efficient encoding for line polar Grassmann codes. Finally, in Section 4 we enumerate some open problems which might be of interest.

2 Projective codes from polar Grassmannians

Let $V := V(2n+1, q)$ be a $(2n+1)$ -dimensional vector space over a finite field \mathbb{F}_q endowed with a non-singular quadratic form η of Witt index n .

The *polar Grassmannian of orthogonal type* $\Delta_{n,k}$ is a proper subgeometry of the Grassmannian $\mathcal{G}_{2n+1,k}$ of the k -subspaces of V whose points correspond to all totally singular k -spaces of V with respect to η .

For $k < n$ the lines of $\Delta_{n,k}$ are exactly the lines $\ell_{X,Y}$ of $\mathcal{G}_{2n+1,k}$ where Y is totally singular; on the other hand, when $k = n$ the lines of $\Delta_n := \Delta_{n,n}$ are sets of the form

$$\ell_X := \{Z \mid X \subset Z \subset X^\perp, \dim(Z) = n, Z \text{ totally singular}\}$$

with X a totally singular $(n-1)$ -subspace of V and X^\perp its orthogonal with respect to η . Note that the points of ℓ_X form a conic in the projective plane $\text{PG}(X^\perp/X)$.

Clearly, for $k = 1$, the geometry $\Delta_{n,1}$ can be identified with the orthogonal polar space $Q(2n, q)$ of rank n associated to η . When $k = n$, the geometry Δ_n is, in some sense, the dual of $\Delta_{n,1}$ and it is called the *orthogonal dual polar space* of rank n .

Define now $W_k := \bigwedge^k V$. The *Grassmann* or *Plücker embedding* $e_k^{gr} : \mathcal{G}_{2n+1,k} \rightarrow \text{PG}(W_k)$ maps the arbitrary k -subspace $\langle v_1, v_2, \dots, v_k \rangle$ of V (hence a point of $\mathcal{G}_{2n+1,k}$) to the point $\langle v_1 \wedge v_2 \wedge \dots \wedge v_k \rangle$ of $\text{PG}(W_k)$.

It is well known that $e_k^{gr}(\mathcal{G}_{2n+1,k})$ is an algebraic variety; furthermore the lines of $\mathcal{G}_{2n+1,k}$, that is to say collections of k spaces all mutually intersecting in a given $k-1$ space are mapped into lines of $\text{PG}(W_k)$.

Denote now by $\varepsilon_k^{gr} := e_k^{gr}|_{\Delta_{n,k}}$ be the truncated restriction of e_k^{gr} to $\Delta_{n,k}$. The image of $\Delta_{n,k}$ under ε_k is the k -Fano variety of the quadric $Q(2n, \mathbb{F}_q)$. For $k < n$, all lines of $\Delta_{n,k}$ are mapped by ε_k^{gr} into lines of $\text{PG}(W_k)$. We observe however that for $k = n$ a line of Δ_n is mapped into a conic in $\text{PG}(W_n)$; see [2] for details.

Given any set of points $\Omega \subseteq \text{PG}(W)$ with W vector space over \mathbb{F}_q , the projective code defined by Ω is a linear q -ary code $\mathcal{C} := \mathcal{C}(\Omega)$ whose generator matrix contains as columns the coordinates of the points of Ω . This code is uniquely defined up to code equivalence. It is well known that the parameters of a projective code are

$$N = \#\Omega; \quad K = \dim\langle\Omega\rangle; \quad d_{\min} = \#\Omega - \max_{\substack{\Pi \leq W, \Omega \not\subseteq \Pi \\ \text{codim } \Pi = 1}} \#(\Pi \cap \Omega).$$

In particular, the study of the minimum distance of \mathcal{C} is equivalent to the investigation of the possible hyperplane sections of Ω .

Projective codes arising from the Plücker embedding e_k of ordinary Grassmannians $\mathcal{G}_{n,k}$ in $\bigwedge^k V$ have been extensively investigated in recent years; in particular, see [12, 13, 11, 8, 9, 7].

In the present note we are concerned with codes $\mathcal{P}_{n,k}$ arising from the projective system $\Omega_{n,k} := \varepsilon_k(\Delta_{n,k})$ given by the Plücker embedding ε_k of an orthogonal Grassmannian.

Main Result 1 ([3]) *Let $\mathcal{P}_{k,n}$ be the code arising from the projective system $\varepsilon_k^{gr}(\Delta_{n,k})$ for $1 \leq k < n$. Then, the parameters of $\mathcal{P}_{n,k}$ are*

$$N = \prod_{i=0}^{k-1} \frac{q^{2(n-i)} - 1}{q^{i+1} - 1}, \quad K = \begin{cases} \binom{2n+1}{k} & \text{for } q \text{ odd} \\ \binom{2n+1}{k} - \binom{2n+1}{k-2} & \text{for } q \text{ even,} \end{cases}$$

$$d \geq \psi_{n-k}(q)(q^{k(n-k)} - 1) + 1,$$

where $\psi_{n-k}(q)$ is the maximum size of a (partial) spread of the parabolic quadric $Q(2(n-k), q)$.

Here $\psi_r(q) = q^{r+1} + 1$ for q even and $\psi_r(q) \geq q + 1$ for q odd.

To provide a sketch of the proof, observe that N is just the number of totally singular k -spaces contained in a $Q(2n, q)$. The dimension K arises from some results on embedding of Polar Grassmannians in [1, 2]. In particular, for q odd the dimension of a polar Grassmann code is the same as that of the corresponding Grassmann code. The estimate on the minimum distance derives from the study of maximal totally singular subspaces contained in $Q(2n, q)$; in particular, for any given fixed k -dimensional totally singular subspace E there are at least $\psi_{n-k}(q)$ generators H_i of $Q(2n, q)$ meeting just in E . In each of the spaces H_i/E it is then possible to apply the well-known result on the minimum distance of Grassmann codes.

As the sketch above illustrates, it has to be expected that the bounds we obtain in Main Result 1 are not sharp.

More recently, in [4], together with A. Pasini, we have been able to fully determine the minimum distance for Line Polar Grassmann codes, i.e. codes with $k = 2$, for q odd.

Main Result 2 ([4]) *Suppose $n \geq 2$ and q odd; then, the minimum distance d_{\min} of the orthogonal Grassmann code $\mathcal{P}_{n,2}$ is*

$$d_{\min} = q^{4n-5} - q^{3n-4}.$$

Furthermore, all words of minimum weight are projectively equivalent.

The proof of this theorem hinges upon the observation that any hyperplane Π of $W_2 = V \wedge V$ corresponds to an alternating bilinear form π on V . In particular, we have $L \in \Pi \cap \varepsilon_2^{gr}(\Delta_{n,2})$ if, and only if, the line ℓ whose image is L is simultaneously totally singular for the quadratic form η and totally isotropic for the (degenerate) bilinear form π . As it might be expected, the forms π giving maximum intersection turn out to have maximum radical and, consequently, maximum number of totally isotropic lines; in the case of ordinary Grassmann codes, all of these forms are equivalent; however, for polar Grassmann codes there are many inequivalent possibilities. Our argument relies upon providing a detailed analysis of these possibilities and bounds on the values which might occur.

Observe that in Main Theorem 1 we have not considered the case of dual polar spaces. We have however determined the value of the minimum distance when $n = k = 2$ and $n = k = 3$, as illustrated by the following theorem.

Main Result 3 ([3]) (i) *The code $\mathcal{P}_{2,2}$ arising from a dual polar space of rank 2 has parameters*

$$N = (q^2 + 1)(q + 1), \quad K = \begin{cases} 10 & \text{for } q \text{ odd} \\ 9 & \text{for } q \text{ even,} \end{cases} \quad d = q^2(q - 1).$$

(ii) *The code $\mathcal{P}_{3,3}$ arising from a dual polar space of rank 3 has parameters*

$$\begin{aligned} N &= (q^3 + 1)(q^2 + 1)(q + 1), & K &= 35, & d &= q^2(q - 1)(q^3 - 1) & \text{for } q \text{ odd} \\ & & \text{and} & & & & \\ N &= (q^3 + 1)(q^2 + 1)(q + 1), & K &= 28, & d &= q^5(q - 1) & \text{for } q \text{ even.} \end{aligned}$$

3 Enumerative encoding

Grassmann linear codes have a very low data rate; as such it is paramount to be able to describe efficient encoding and decoding algorithms acting locally on the components. To this aim, in [14], an efficient algorithm for enumerative coding of Grassmannians is introduced; see also [10] for some improvement. Their work is based upon the approach of [6] which requires to determine the number of subspaces whose representation begins with a given prefix.

The techniques of [14] cannot be directly applied to polar Grassmannians, as the value of the quadratic form η must also be tracked. In [5] we introduced an enumerator algorithm for Line Polar Orthogonal Grassmannians of complexity $O(q^2 n^3)$.

Using this algorithm, we can provide both efficient encoding and efficient error correction for Polar Grassmann codes. More in detail,

1. It is possible to fully locally encode any Line (Polar) Grassmann code. Indeed, given a message \mathbf{m} it is easy to determine an alternating form $m(x, y)$ acting on the vector space V . For any position i in $\mathcal{P}_{n,2}$, the value of the codeword corresponding to \mathbf{m} is just $m(A, B)$ where A, B are the two generators of the line with index i in $Q(2n, q)$ taken in Row Reduced Echelon Form.
2. There is also a form of local error correction which can be obtained by exploiting the geometry. Indeed, given an index position i , let ℓ_i be the corresponding totally singular line. Then, it is possible to study the bilinear forms induced by a codeword \mathbf{c} on the totally singular planes passing through ℓ_i and use this information in order to recover the value c_i is supposed to have.

The details are contained in [5].

4 Open problems

We conclude this survey, by presenting some open problems.

- a) *Bounds for the minimum distance of Orthogonal Polar Grassmann codes for $k > 2$.*
- b) *Generating sets of minimum weight*
In the case of line polar Grassmann codes the minimum weight codewords are all projectively equivalent. Do they constitute a generating set for the code ? If not, what is the dimension of the subcode they span?
- c) *Spectrum of low weight codewords*
In [4] we constructed several classes of codewords (depending on some parameters) in order to explicitly estimate the minimum distance. The same construction can be used to produce several codewords of different weight. Do they provide an exhaustive list of all possible small weight codewords? What about the weight enumerator?
- d) *Higher weights*
Determine at least some of the higher weights of line polar Grassmann codes.
- e) *LDPC codes*
Consider the incidence matrix H of the design of hyperplanes of $\bigwedge^k V$ and the Grassmann embedding of a polar Grassmannian $\mathcal{D} := \varepsilon_k(\Delta_{n,k})$. What can we say about the binary code \mathcal{C} with parity check/generator matrix H ? Some low weight codewords of \mathcal{C} correspond to hyperplanes with *maximum* intersection with \mathcal{D} ; are these the codewords of minimum weight? Is this code generated by its minimum weight codewords? What is the dimension of \mathcal{C} (i.e. the 2-rank of G) ? What about p -ranks for $p > 2$?
- f) *Network coding with polar Grassmannians*
The Grassmann graph arising from Polar Grassmannians has diameter strictly larger than that of the corresponding projective Grassmannian. Can this be exploited in order to offer better correction capabilities in the case of random network coding?

References

- [1] I. Cardinali and A. Pasini, *Grassmann and Weyl Embeddings of Orthogonal Grassmannians*, J. Algebr. Comb., **38** (2013), 863-888.
- [2] I. Cardinali and A. Pasini, *Veronesean embeddings of dual polar spaces of orthogonal type*, J. Combin. Theory Ser. A. **120** (2013), 1328-1350.
- [3] I. Cardinali and L. Giuzzi, *Codes and caps from orthogonal Grassmannians*, Finite Fields Appl. **24** (2013), 148-169.
- [4] I. Cardinali, L. Giuzzi and A. Pasini, *Line Polar Grassmann Codes of Orthogonal Type*, preprint.
- [5] I. Cardinali and L. Giuzzi, *Enumerative Coding for Line Polar Grassmannians*, preprint.
- [6] T. M. Cover, "Enumerative source encoding," *IEEE Trans. Information Theory*, vol. IT-19, no. 1, pp. 73-77, 1973.

- [7] S.R. Ghorpade, K. V. Kaipa, *Automorphism groups of Grassmann codes*, Finite Fields Appl. **23** (2013), 80-102.
- [8] S.R. Ghorpade, G. Lachaud, *Hyperplane sections of Grassmannians and the number of MDS linear codes*, Finite Fields Appl. **7** (2001), 468-506.
- [9] S.R. Ghorpade, A.R. Patir, H.K. Pillai, *Decomposable subspaces, linear sections of Grassmann varieties, and Higher weights of Grassmann codes*, Finite Fields Appl. **15** (2009), 54-68.
- [10] Y. Medvedeva, "Fast enumeration for grassmannian space," in *Problems of Redundancy in Information and Control Systems (RED), 2012 XIII International Symposium on.* IEEE, 2012, pp. 48-52.
- [11] D. Yu. Nogin, *Codes associated to Grassmannians* in Arithmetic, geometry and coding theory (Luminy, 1993), de Gruyter (1996), 145154.
- [12] C.T. Ryan, *An application of Grassmannian varieties to coding theory*, Congr. Numer. **57** (1987), 257-271.
- [13] C.T. Ryan, *Projective codes based on Grassmann varieties*, Congr. Numer. **57** (1987), 273-279.
- [14] N. Silberstein and T. Etzion, "Enumerative coding for Grassmannian space," *IEEE Trans. Inform. Theory*, vol. 57, no. 1, pp. 365-374, 2011. Available: <http://dx.doi.org/10.1109/TIT.2010.2090252>